

MEI Encryption Review

Schedule, Statement of Work and Deliverables

RAND

October 28, 1996

A. Background and Scope

Matsushita Electric Industrial Company, Ltd. (MEI) has developed an encryption system for use with DVD players. Before distributing their intellectual property in this medium, the major studios, represented by the MPAA, would like to evaluate this encryption system with respect to risks associated with intellectual property piracy. To assist in this endeavor, RAND will bring together a review team of encryption and information technology specialists from the proposed RAND Media Research Institute (MRI). Within a two-week time frame in November, the team shall review the MEI encryption proposal with respect to the degree of security it offers, potential weaknesses in the system and possible methods to increase the level of the security it provides.

B. Statement of Work

RAND shall conduct a review of the proposed MEI encryption system by addressing the following questions:

1. Does the system provide a reasonable defense against home piracy?
2. Could the system be unintentionally compromised?
3. Would a system compromise result in small-scale or catastrophic losses?
4. Is the system flexible in terms of future modifications and cross-industry use?
5. Does the system comply with federal regulations controlling encryption technologies?

A letter report will be generated and delivered to the MPAA in late November that documents the panel's finding and their basis. To the extent possible, the report shall not discuss technical details of the MEI encryption system, such as the algorithm, coding, or formulas.

FOX 00438

AEC

C. Approach

In order to complete its review, the RAND team will use the following approach in addressing each of the questions posed in the statement of work.

1. Does the system provide a reasonable defense against home piracy (yes/no)?

The team will qualitatively assess the degree of security offered by the encryption system in terms of its underlying algorithm and planned implementation. Because of the inherent complexity of the problem, it is impossible to give a rigorous analytical determination of the level of effort necessary to defeat any non-trivial system. On the other hand, the relative degree of difficulty could be generally assessed, and weaknesses in the system could be identified based upon expert insight and experience in design practices.

2. Could the system be unintentionally compromised (yes/no)?

From the above assessment, the team will judge whether the encryption system could be compromised without specific intent. Such a judgment would indicate the probability that violators of the system could be prosecuted and convicted to the full extent of the law.

3. Would a system compromise result in a) small-scale or b) catastrophic losses?

Assuming that the system could be compromised, the team will gauge the relative extent of the potential damage. Could such a compromise result in one unauthorized copy of a product? One thousand unauthorized copies of a product? Unlimited unauthorized copies of an entire product line? Such an assessment should help the studios understand the full scope of the economic risks involved.

4. Is the system flexible in terms of future modifications and cross-industry use (yes/no)?

To the extent possible, the security architecture should be open to modifications and upgrades, as better algorithms and methods are developed. Furthermore, the architecture should be acceptable for use within other industries, such as telecommunications and personal computers. The team will determine the openness and flexibility of the system.

5. Does the system comply with ITAR rules (yes/no)?

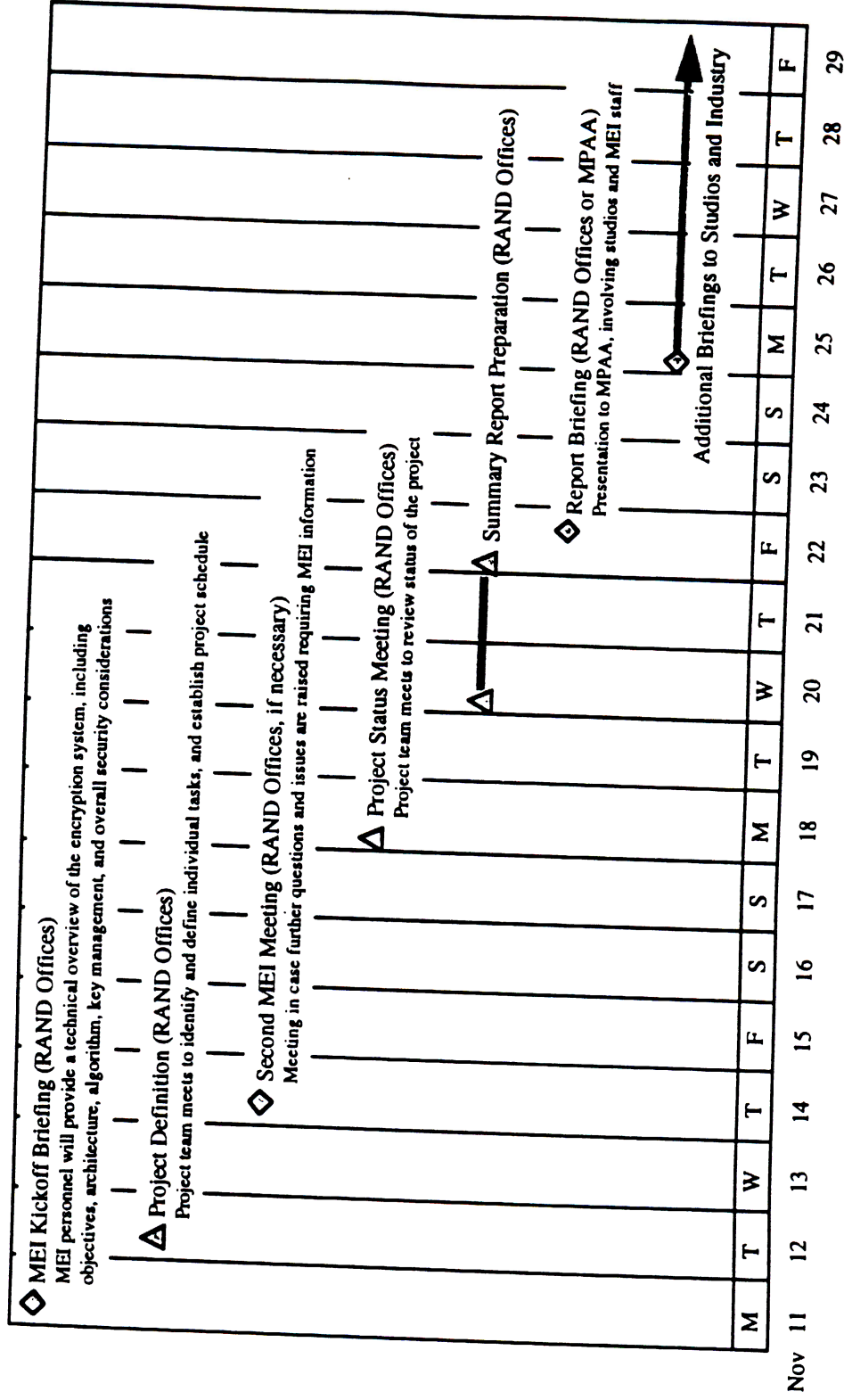
For export from the United States, encryption systems must comply with federal regulations which categorize certain types of algorithms along the same lines as munitions. However, the regulations have been undergoing modifications to adapt to new developments in technology. The team will consider such issues to ensure that the encryption system is not blocked by such regulations.

In addition to these technical issues, the RAND team may also consider and comment upon the following topics: integration of the algorithm with the protocols, key management, key expiration, and the effectiveness of the method and administration of licensing of the technology.

D. Schedule

The Table below provides an example schedule for the proposed MEI encryption review.

Project Schedule*



* This schedule assumes that selected items will be completed prior to the start of Review Team efforts; these include...

- MEI-RAND Non-Disclosure Agreement (signed no later than November 5)
- RAND data requirements list provided to MEI (November 6)